single authentication procedure can be reasonably understood as re-running an authentication and key agreement procedure already run between a mobile node and an authentication server. The Examiner is requested to specifically identify by number the numbered step in column 12 where Haverinen describes re-running the authentication procedure previously executed for that request.

The Examiner admits that Haverinen does not use the term "re-running." For this explicit term, the Examiner relies on newly-cited Weschler at column 16, lines 1-12. Weschler describes at column 15, line 65-column 16, line 12, the following:

> The context object 614 supports client certification methods. The certification methods 622 allow the sender to digitally 'sign' the control data, thereby authenticating its origin and content, and increasing the security of the client/server communication. Basically, signing a message is a two step process. First, the messages run through a hashing algorithm which returns a message digest number. A digest number is generally a fixed length number unique to the hashed message. If the message is altered in anyway, re-running the hashing function on the altered message returns a different message digest number. Next, the sender encrypts the digest message number with his or her own private key and attaches the encrypted digest number to the end of the message. (emphasis added).

The way in which Weschler uses the term "re-run" in the quoted text above is not relevant to the way the term is used in claim 23. A re-run in Weschler occurs for a different message, i.e., an altered message.

The Examiner suggests on page 5 of the final office action that in Weschler "basically, signing a message is a two step process, run through a hashing algorithm and re-running the hashing algorithm." This paraphrase by the Examiner simply does not accurately characterize what the Weschler passage describes. Weschler's encryption is a two step process. The first step is to run the message through a hashing algorithm to return a message digest number. The second step is to encrypt the message digest number with a sender's private key and attach the encrypted digest number to the end of the message. There is no disclosure or suggestion that the hashing algorithm is run again. Thus, there is no suggestion in Weschler of re-running an authentication procedure. All Weschler teaches is that a procedure involves a unique digest number.

Accordingly, even if the combination of Haverinen and Weschler could be made, for purposes of argument only, that combination fails to disclose or suggest "re-running and authentication and key agreement procedure defined for the radio communication network, between a mobile node and an authentication server of the radio communication network," as recited in independent claim 23. A similar feature is also missing from apparatus claim 30. Moreover, the office action does not set forth a proper reason for combining Weschler with Haverinen. All the Examiner contends is that it would have been obvious to implement Weschler in Haverinen "in order to create a secure data transfer through a re-authentication and key agreement process." In other words, the Examiner is simply parroting back the claim language that is actually missing from both Haverinen and Weschler. This parroting back of the claim language is not a reasonable basis for combining the two references. At best, it is impermissible hindsight.

The application is in condition for allowance. An early notice to that effect is earnestly solicited.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: ____________________
John R. Lastova
Reg. No. 33,149

JRL:maa
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100